DEEPONION WHITE PAPER

Written by the DeepOnion Development Team

V 2.0

ABSTRACT

Our Whitepaper defines the goals of the project and examines DeepOnion's Vision. We conduct a thorough assessment of the current ecosystem of cryptocurrencies by describing the blockchain innovations which back up this new cryptocurrency. It also presents how DeepOnion seeks to solve the flaws identified within the current system by implementing our latest technology.

Secondly, we give a detailed explanation of the introduction of our core technologies in regards to their technical specification, rationale, testing, implementation, and deployment. Lastly, we provide a clear path to success by outlining our vision for future improvement to the DeepOnion project in creating anonymous payment ecosystem that guarantees security and privacy.

Index Terms
—

Cryptocurrency, Anonymity, Privacy, TOR, Smart Contracts, DeepVault, ONION, DeepSend.

INTRODUCTION

DEEPONION is referred to as a hybrid cryptocurrency as it implements the x13 proof of work (POW) and the proof of stake (POS) algorithm. The Onion Router (TOR) protocol is implemented and integrated natively within the TOR [2] network. This ensures the security and anonymity of all peer-to-peer connections.

The primary purpose of DeepOnion is to protect the privacy and identity of an individual by creating a payment platform that is instantaneous, scalable, secure, anonymous and untraceable.

DeepOnion minimizes the likelihood of identification by both legal and illegal entities to promote the anonymity and privacy of cryptocurrency users by incorporating anonymity-centric networking protocols and industry-leading cryptography.

DeepOnion also seeks to implement DeepSend and other innovative and proven blockchain technologies such as Stealth Addresses, which would make it difficult to violate our users' privacy.

DeepOnion, a privacy focused cryptocurrency.

We believe privacy is a right. DeepOnion allows users to send untraceable payments with ease. Integrated with the latest TOR, OBFS4, and Meek for maximum privacy.

Download Now

Latest TOR Integration

This allows you to mask your IP and location by using the TOR network nodes.

Instant Confirmations

Send and receive instant payments worldwide. You no longer have to wait several minutes or hours to receive a payment confirmation.

Untraceable Payments

With the built-in Stealth Address feature, you can send untraceable payments.

Multiple Layers of Protection

DeepOnion has several layers of privacy including the latest version of Tor, obfs4, meek, stealth addresses, and upcoming DeepSend.

DeepSend is our hidden payment technology that was primarily designed to protect the senders' identity and obfuscate payment transactions.

With the implementation of many layers of security such as Stealth Addresses, a technology that safeguards the identity of the receiver, the TOR protocol was natively integrated to ensure that all the connections within the DeepOnion are protected. DeepSend also offers security and anonymity of transactions as mentioned earlier.

DeepOnion makes the balanced research or tracing of the coin movement impossible throughout the DeepOnion network or even with social engineering. The primary aim of DeepOnion is to offer an anonymous platform that operates over a secure and private network.

Cryptocurrency users can now transfer their wealth freely without observation and scrutiny by legal authorities and malicious attackers.

DeepOnion's Future Vision

DeepOnion seeks to become a premier hybrid cryptocurrency that guarantees privacy and anonymity of its users by introducing the novel blockchain technologies and improving the current state-of-the-art. The development has integrated the latest privacy standards into DeepOnion's technology stack. The latest TOR protocol was incorporated to ensure that the finances of our community members remain anonymous and secure in every aspect. We have gone an extra mile by adding VoteCentral, a voting mechanism that allows democratic and anonymous representation of the future development of DeepOnion.

It is our belief that nobody should have their finances or identity scrutinized by financial authorities, Government entities or any other individual or group because privacy is an inherent right. We are working to offer the latest technology that will protect the user's privacy.

Security technologies are dynamic and because they evolve over time, we include a variety of actual technologies that would make it difficult for both legal and illegal parties to invade the security of DeepOnion users.

It becomes very difficult for anyone to breach the walls of privacy because of our massive protocols in our network.

This has been facilitated through the integration of the blockchain technology that operates on the DeepOnion network. DeepOnion is always under constant development since it is an evolving project that attempts to meet the dynamic demands on privacy, security, and technology to maintain a competitive edge of the advancement in cryptocurrency.

The essential element is that DeepOnion is a community; a family that believes in financial obfuscation and online privacy. The critical component to achieving success in DeepOnion project is having a core community and we take pride in the thousands of people who promote and support us in such a short period of time. We become stronger when we work together and together, we are DeepOnion.

CURRENT PROBLEMS IN CRYPTOCURRENCY

Currently, Bitcoin (BTC) is the dominant cryptocurrency with a market share and a market cap of 37.6% and $368 billion respectively, despite the fact that it is experiencing inherent flaws. Most fears in the crypto-world are not only exacerbated by wild price fluctuations, but also lack of security and privacy of the crypto-investors. Our point of the argument lies in the elaboration of what is lacking in Bitcoin and other major cryptocurrencies such as Ethereum, Litecoin, and Ripple, and how DeepOnion seeks to solve these issues.

Privacy and anonymity

Bitcoin [1] is built upon an immutable blockchain, SHA-256 bit encrypted that is publicly available and distributed over a decentralized network supported by wallet users and miners. In situations where a human identity is linked to a wallet address through a commercial vendor or a crypto exchange, it is compromised irrevocably with regards to privacy. The anonymity of a user can never be retrieved without generation of a new one and loss of the remaining BTC linked to the same address. This can be compared to having a public record of your bank statement indicating all available transactions that can be seen by everyone.

We witness the empirical demonstration of this phenomenon in an event where an individual considers exchanging Bitcoin into the FIAT currency through an online exchange and vice versa. It is possible to conceptualize a typical scenario as:

- An account with the exchange is created by the user who registers his or her personal details that would facilitate the currency exchange.

- An exchange generates the BTC address which is connected to your personal identity.

- The funds are sent by the user from their FIAT bank account (or BTC wallet) to their identity verified exchange wallet.

- A trade is then performed by the user

Unfortunately, the outcome of the above process is that your BTC address that was once anonymous is now linked irrevocably to your personal identity. This implies that the exchange is in a position to exactly verify the number of BTC you have in all the addresses (i.e. your newly created address and your once anonymous BTC address). Furthermore, they can verify to whom you are receiving or sending BTC.

In circumstances where the BTC is required to share the details of their customers to Government bodies or law enforcement agencies, then they also get to know your identity as well as the number of BTC you have in your wallet. The same applies to the addresses of the persons you have been interacting with over the past transactions.

The recent Wannacry ransomware [10] outbreak that saw millions of computer systems infected throughout the world is one of the empirical demonstrations of the ability to track this blockchain. The ransom demanded to decrypt the files of an infected machine requested in BTC which made the wallet address public and also available for tracking. It became increasingly difficult in the following months for the responsible group to exchange their BTC for the FIAT currency because the BTC could be tracked within the blockchain every time it moved to another wallet. Given that this was a criminal act, many would argue that it is a positive feature but let's consider the following scenario which was perfectly legal.

Try to imagine yourself during a tender agreement but in a negotiating position. If your financial investments could be tracked by your competitor by obtaining a list of your contractors and suppliers through blockchain exploration, how would it be? This would definitely undermine your negotiating position as it provides your competitor with valuable insights into your finances.

It could also result in other outcomes such as a corporate takeover, outbidding and full disclosure of your previous business relations and investments.

For most businesses, this could be catastrophic and perhaps one of the primary reasons major institutions doesn't adopt BTC because privacy is a fundamental principle when it comes to financial operations. (Actually, it is information that is mandated in several jurisdictions).

Therefore, there is clarity in the fact that the level of privacy adopted by BTC makes it fully inadequate for mass adoption. We can now make our conclusions on the "anonymous" nature of Bitcoin that is quoted often to be a fallacy in the eyes of its users.

Anonymity

Another area of weakness for BTC is anonymity since node traffic is often sent in a fashion that is unencrypted. The peer addresses of BTC are clearly visible Internet Protocols that present a prime opportunity for consequently network interruptions and targeted attacks.

This data is obtained trivially in any of the freely available BTC wallets through the 'getpeerinfo' command. It is considered a bad practice and unsecured way to disclose your computer wallet's public IP address involuntarily without having any adaptive security appliances (or adequate perimeter defenses).

Some of the potential risks involved include the ability to link the user's IP to their wallet address and disclosing further the coin holder's identity. This could result in an intelligence-based attack that is more sophisticated.

Therefore, it is an imperative action to protect the IP address of the client's wallet to safeguard your financial assets as well as protect your personal identity. The anonymous TOR IP addresses are some of the implementations made by DeepOnion to specifically mitigate these risks.

Scalability and Speed

BTC demands that all previous blocks within the blockchain are verified cryptographically by all nodes on the network. This requires significant storage space and computing power in regards to the blockchain size (due to the number of transactions and age of BTC). It also requires a significant amount of time that would allow processing of the entire chain. BTC solely relies on the SHA-256 based x13 proof of work (PoW) to mint new coins and process blocks.

There is also a speed limit on how the transaction takes place which is proportionate to the difficulty currently configured by the design. A single block at present has a high degree of variability and has a confirmation time of 350 minutes. Most services often require a minimum of 6 confirmations for verification. This means that to send or receive a payment, you are likely to spend at least 35 hours which rules it out as a perfect payment system in the modern world.
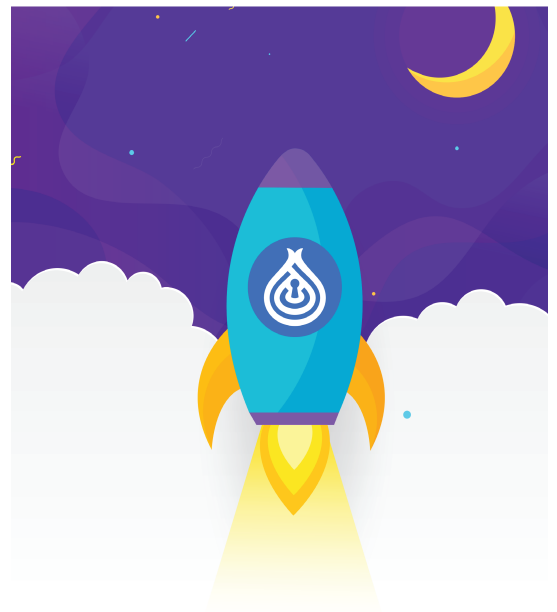
A Misleading Market Cap
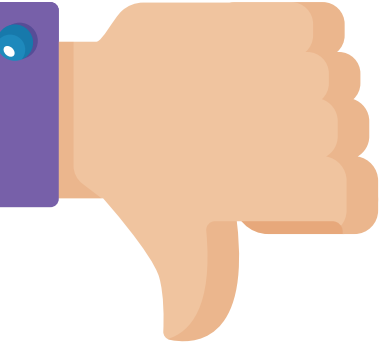
The market cap for digital currencies can be misleading in cases where units that were included in the calculation of the market cap are not easily available for trade. The Auroracoin is the best example of a digital currency with an inflated market cap. It was reported to have a market cap of more than $1 billion but in reality, the bigger portion wasn't available for anyone.

Another asset that has been accused of overvaluation is the XRP token of Ripple because the vast majority of the XRP in existence was owned by the company. DeepOnion attempts to solve the problem of misleading marketing cap as we share openly the number of ONIONs mineable to by the public. 18 million ONIONs will be distributed freely via airdrop to the community. This forms about 90% that have been set to be premined in the genesis block while 2 million ONIONs is the number that will be mineable by the public.

Cost of Transaction

Some cryptos including Bitcoin and Ethereum might be the leading in the industry but are too slow when it comes to processing for everyday commercial use. For instance, Bitcoin miners can handle 3 to 7 transactions per second compared to the visa which has the ability to process over 24,000 during the same period. The resources required to verify transactions in Bitcoin and Ethereum are at times cost-prohibitive. BTC produces a transaction fee that sums up to $25 during the peak periods. This renders it unfit for performing cheaper or affordable transactions compared to the latest booming cryptocurrencies such as DeepOnion.

DEEPONION'S VISION

DeepOnion has a solution to most of these problems since a myriad of technologies has been integrated into the core stack. The TOR network controls the entire network (see 6.1) which makes it very difficult to ascertain the identity of a user without compromising huge segments of the TOR network. This is a process that can be interfered with further with the use of VPN (Virtual Private Network) solutions. This implies that the geographical position of a DeepOnion user is almost impossible to identify or locate.

On the other hand, there is no encryption on the BTC traffic which is the specific rationale behind proposition of the BIP 151. This allows an IP address linked to the BTC network to be determined by packet snooping. In situations where BTC is illegal in your country's jurisdiction, it could lead to legal ramifications.

Furthermore, it shows that you are using BTC and discloses the people you are connecting to. This is information every user would choose not to disclose or keep away from the eyes of the public.

DeepOnion will adopt various industry-leading standards from the field of network security and cryptography to offer security at multiple levels. The diagram below highlights our multi-layered approach to anonymity and security:
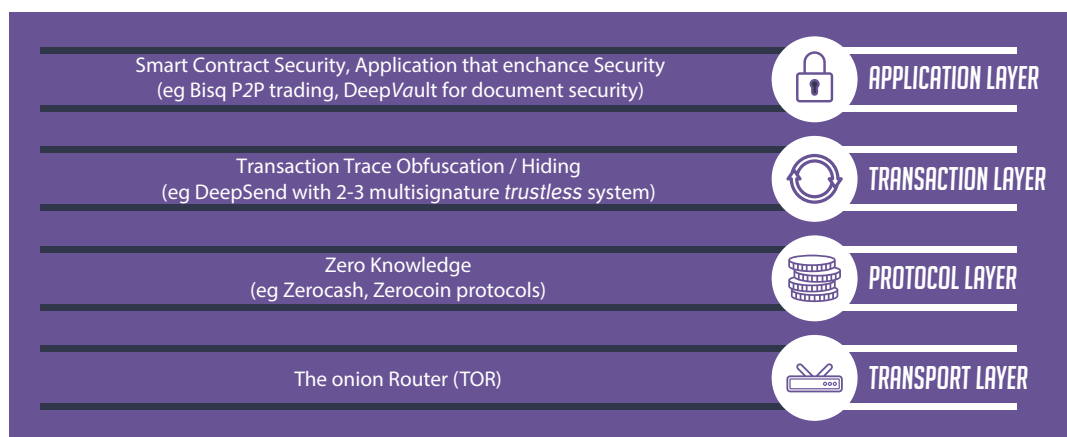

Fig. 1 DeepOnion's Multi-layered Security Model

We integrate the TOR protocol at the transport layer to secure and create anonymity of the network traffic in between the nodes.

We have included the addition of the protocol layer [11] (zero-knowledge proofs) in our roadmap to obfuscate the traces of ONION transactions to every user but the sender. However, we provide sufficient and non-sensitive evidence for the occurrence of the transactions. The origins of a transaction will be hidden further when we implement our DeepSend technology, based on multi-signatures [12] and completely trustless system.

The final stage of anonymity and security is offered by the application layer through the adoption of services such as marketplaces, decentralized exchanges and other services that only operate in a manner that is anonymous, decentralized, secure and cryptographically verified. These measures will ensure that the multi-layered platform gives the absolute best privacy.

(The confirmation of all details will be provided at a later date).

The Roadmap of DeepOnion

The DeepOnion Roadmap as illustrated in (Fig.2) gives a great overview of features that are yet to be implemented within the project and their estimated period of implementation. Although it is our endeavor to keep up with these deadlines, it is not unpopular for a project of this scope and magnitude to slip. To mitigate these risks effectively, we came up with contingency plans and hiring of additional members of our development team when necessary. All delays will be disclosed publicly in any event that it occurs.

THE FEATURES
OF DEEPONION

This section only highlights DeepOnion's features before we provide a more detailed analysis in (Section 6). We introduce the coin specifications of Deep-Onion, its fair process of distribution and other details relating to the formulation and tools of support to the DeepOnion community.

ROADMAP

JULY 2017:

-DeepOnion Pre-Announcement (completed)
-DeepOnion Formally Launched, Airdrop details published
-DeepOnion Blockchain Starts, Mining Starts
-Website Launch (https://deeponion.org)
-Signature Promotion Applications Ready - People can sign up for free ONION airdrops
-Announce DeepOnion Bounty Programs (Translation, Twitter, etc.)
-Signature Campaign Start, First Airdrop Starts - 12.5 Million ONIONs will be distributed freely in about 40 airdrops/distributions
-DeepOnion Forum Launches

2017 Q3:

-DeepOnion Trades at Exchanges
-Twitter Campaign Starts
-Facebook Campaign Starts
-Introductory Youtube Video Campaign Starts
-Release Paper Wallet and Brain Walle

2018 Q1:

-The release of the Official DeepOnion White Paper.
-Launch Mobile Device Wallets (Android)
-Launch of DeepOnion VoteCentral - ONION holders can vote on new developments and bring up own ideas for future implementations.
-Hiring a public Hero for more videos and marketing.

2017 Q4:

-The Launch of DeepVault - A revolutionary one of a kind service.
-Our SEM experts begin showing ads (new videos and content) to people both new and experts at full speed!
-(Popular Search Engines Organic SEO and paid marketing)

2018 Q2:

-Free airdrop/distribution completes, all 12.5 million coins will be freely distributed.
-More Exchanges trade-able for ONIONs
-More Shopping Sites accepting ONIONs
-DeepVault Web App
-ONION accepted Games

2018 Q3 AND LATER:

-Support Zero Knowledge protocol
-The Launch of DeepSend - our next level in blockchain anonymity in crypto world
-Supporting Smart contract
-Main Stream Media Actions
-DeepOnion Academy - Teaching the world about blockchain and cryptocurrencies
-Trezor Wallet Compatibility
-Smart Contracts
-And beyond - The community will take the lead and define new features and the direction of DeepOnion

DeepOnion

Fig. 2. The DeepOnion roadmap
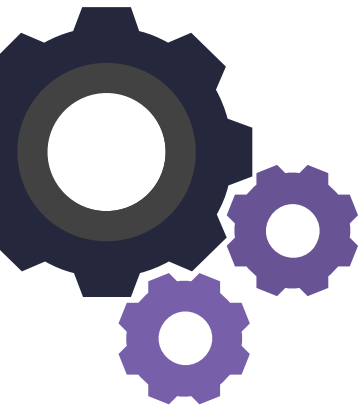
Specification

As we mentioned earlier, DeepOnion is a hybrid cryptocurrency with the PoS and PoW algorithms. Its emission model is recorded at 25 million ONIONS in more than 10 years. Here is the detailed elaboration of the specifications mentioned above;

- 5 confirmations per transaction
- 50 confirmations per block minted
- 18 million ONIONS will be distributed freely via airdrop to the community. This forms about 90% that are set to be premined in the genesis block.
- The number that will be mineable by the public is 2 million ONIONs.
- RPC Port: 18580 – Connection port: 17570.

Proof of Work (POW)

Proof of Work is a protocol that aims at preventing cyber-attacks that could result in multiple fake requests by exhausting the resources of a computer system. It is a concept that has been around even before Bitcoin came into existence. Proof of Work is a requirement that that defines an expensive computer calculation well known as 'mining'. It serves to verify the legitimacy of transactions as well as avoiding double-spending. It also aims at creating new digital currencies by offering rewards to miners for the previous tasks performed.

Features;

- X13 algorithm
- 8 ONION per block will be the initial payout
- 240s block target
- Difficulty retargeting each block
- The payout of the POW will be halved each year until where it remains 1 ONION.

Proof of Stake (POS)

Proof of Stake is a different way of validating transactions while achieving a distributed consensus. Although it serves the same purpose as the Proof of Work, it uses a different process to complete its task. There is no block reward in the PoS system and thus the transaction fees are taken by the miners. One of the biggest advantages of using the proof of stake is that it has a high energy efficiency compared to the proof of work.

Features;

- 60s block target
- Difficulty in retargeting each block
- The interest of PoS will be variable per year:
- 10% 1st year, 5% the second year and 1% in the subsequent years.
- 24 hours minimum holding time before the generation of PoS.

Why is Proof of Stake more preferred?

- It doesn't require high electricity consumption to keep the blockchain secure.

- It is not necessary to issue very many coins to motivate participation of users in the network because of the lack of high electricity consumption.

- Proof of stake allows for a wider range of techniques that deter centralized cartels from arising using game-theoretic mechanism.

- It has reduced risks of centralization because the economies of scale are not a major issue.

- A lot of money is required to attack the system because they will have to allocate a sizeable amount of money when planning an attack. They tend to suffer the attack even if they collect a sizeable amount of money because they will have upset the stability of cryptocurrencies.

x 13 Algorithms

Just as the name suggests, the x13 algorithm utilizes 13 rounds of hashing in combination with other 13 different hash-functions (This includes prominent names such as bmw, Blake, jh, skein, groestl, cube-hash, keccak, and luffa.) All these make it the most secure algorithms in the cryptography of the modern era. This algorithm benefits from a high level of flexibility to allow for the selection of specific hash functions.

It is an added advantage because the adoption of new algorithms can be done in light of collisions [13] that have been identified in a particular algorithm. 13 hashing functions by its very nature are inherently more secure compared to the SHA-256, a traditional single algorithm used by BTC.

Emission Model

- The DeepOnion's emission specification is as follows;
- 240 seconds PoW block target; which translates to 15 blocks in an hour and 360 blocks in a day.
- Initially, 8 ONION is comprised in every block.
- This is a payout that halves each year and thus the number of PoW coins that are minable will be:
- 365 x 360 x 8 x (1 + ½ + ¼ + 1/8 + ...) = 2,102,400
- Therefore 2,102,400 will be the total number of PoW coins (This includes the 18 million that were pre-mined at block 1).

The generation of PoS usually occurs at 10% during the initial year. The second year will be 5% and all the subsequent years will be at 1%. It is estimated that the total number of ONIONs generated over the space of 10 years will be 25 million approximately.

Network Model
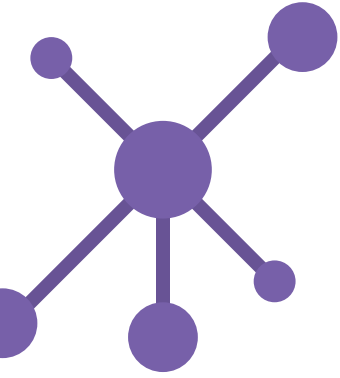
DeepOnion's network is founded upon the TOR network which provides a method of transaction that is anonymous and highly secured. The users of DeepOnion usually communicate via the TOR addresses, e.g. bb3ebyhgfkj3-jzfd.onion. These onion addresses are usually self-authenticated which implies that the address itself gives a cryptographic proof of the service identity. This, in turn, prevents attackers from spoofing the address. There is a multitude of security benefits that arise when the TOR is integrated into the stack of DeepOnion's technologies. It includes;

- Additional privacy on the device that stored the DeepOnion wallet (Your IP becomes untraceable and anonymous).
- Cryptographic verification that affirms the genuineness of the network you connect to.
- Freedom from network surveillance and oversight
- The impossibility for your client being blocked by a particular address.
- Tamper-proofing through encryption and enhanced communications integrity.

Distribution

It is crucial for a new cryptocurrency to have a fair distribution when looking for mainstream adoption. DeepOnion seeks to meet this requirement by offering an additional bounty programme as well as free airdrops. [Appendix A contains the specifics of the airdrop].

The reasoning behind this technique is that most people fold. The holding of the coin can be emphasized with a 40-week airdrop because owners who have received their airdrop previously gain trust in the distribution model. This makes them wait until completion so that their accumulation can be maximized.

The future rewards are offered by the PoS for people who are ready to hold. New users are getting prime opportunity to participate due to the longevity of the campaign which boosts the number of DeepOnion users within the community who are holding ONIONS. A tapered emission of the distribution of airdrops ensures that the number of airdropped coins increases as the number of participants also grows [See Appendix A].

The holding of a large number of ONION occurs within the bounty wallets and development to be utilized when additional recruitment becomes necessary. It can either be as an extra developer venture or as an advertisement. The collection of bounties is done voluntarily when the community members complete goals that have been set by the development team.

Distribution

This distribution model received initial criticism which hypothesizes a situation where a Developer dumps their coins after meeting a critical price. However, it is necessary to put emphasis on the method in which the risk is mitigated.

- 2million ONION is held by the founding members of DeepOnion. Its percentage of the overall ONIONs distributed lies within the successive airdrop of each week (airdrop completed at the time of writing).
- There is a low current volume that prevents a scenario where 'dumping' occurs. The airdrop distribution method facilitates holding which in turn leads to low numbers of ONION during a particular exchange.
- This is an open-source project (excluding the currently secured DeepVault that is yet to be released in due course). There will be a possibility of working with minimal disruption given the skill set and size within the community.
- The work ethic of the development team is categorically denied by a dump of this nature and the same applies to the future vision of DeepOnion's ecosystem.

Community

The strength of DeepOnion lies in reputation and support of its massive community network. Most cryptocurrencies usually fall short of the mainstream adoption because of their lackluster promotion and small user base. We understand clearly how essential the social aspect can be from the time of inception since the formation of the community is done with utmost importance. Furthermore, we introduced a voting platform to ensure that the future of the project can be shaped by DeepOnion users.

We have created a plethora of supporting technologies and social media outlets to ensure that this requirement is fulfilled. Our official forum is the most notable and is available at https://deeponion.org. The platform boasts unique features that are not available on other forum software and gas always been the heart of our community. We are also dominant on other proprietary platforms such as YouTube, Reddit, and Twitter that are used in our advertisements. The community projects also boast having a large following which shows the great support by our followers.

DeepOnion has had an extremely successful strategy and currently, we have one of the most popular and largest threads that have been established on the BitcoinTalk.org forums. We will continue to pursue this social outlet because its level; of exposure is highly beneficial. Most importantly, it reflects the sentiments of people towards the DeepOnion project and their willingness of participation, support and involvement.

Forums

Our community hubs are the official forums for DeepOnion and are used in promotional events to coordinate our 'call to arms' as well as a social interaction platform. Exceptional growth has been realized in the official forums over the past 6 months and is one of the primary rationales behind the continued success of DeepOnion.

You can get our forums at https://deeponion.org and everyone is free to register. To find out more about DeepOnion please visit our official website as you can ask any questions you may have about our excellent, friendly community. Most likely, you will be surprised by the number of diverse and talented individuals we incorporate into our community. You are always welcome to be part of our journey to success.

Stealth Addresses

The DeepOnion Development team has taken the level of privacy to the next level by introducing Stealth Addresses. As the name suggests Stealth Addresses are used to create an address that cannot be traced by the regular explorers because it protects the privacy of the one receiving the payments. The sender and the receiver are the only sole parties that will be aware of the true identity of each other (and just for the sender, because next time it will create another unique address).

However, no other third parties to the transaction will have a hint about what transpired. DeepSend has created a way of splitting the transaction into random nodes that would make it very difficult to trace the sender. This can only happen when all the transactions are completely untraceable.

To understand more about the stealth addresses, let's consider the following scenario;

- The recipient generates a key pair (private/public)
- The recipient then allows everyone to know more about the Stealth Address (Public key) but keeps the private one secret.
- The sender takes the public key or the Stealth Address and then adds a random value to it so that it can generate a normal address – so cool, right?
- Next, they load onions into this address.
- The sender encrypts the private key (the random number from above) together with the normal address and puts this data into the blockchain (all this data appears as gibberish to other clients who do not possess the private key).
- The recipient then uses his private key to decrypt the data and voila – he gains access to the normal address as well as the ONIONs.

Benefits of stealth addresses

- They add more safety, trust, and privacy to the users.
- The destination of where a payment was sent can only be concluded by the sender and the receiver
- No third party will be aware of any payments or transactions that you received from other people.
- The blockchain cannot make a correlation because you send and receive payments using separate and unique addresses.
- Since no third party is involved in the transaction, they won't know anything about the payments more so if there is no direct communication between the receiver and the sender.

Atomic Swaps

Atomic swap is another upcoming feature that doesn't require a trusted third party when exchanging one cryptocurrency for another. Trusted third parties used to be a necessity in the traditional cryptocurrencies when performing a cryptocurrency exchange. This was done to prevent one party from losing part of their currency without receiving another currency in return.

From a theoretical point of view, the Atomic Swaps would create a solution for the need of a decentralized exchange. Although scalability may be a concern, the development team is working hard enough to ensure that everything is put into consideration to allow for more privacy when implementing this technology.

Smart Contracts

The support of Smart Contracts is another feature that DeepOnion plans to have in the near future. The smart contract is hash time-locked and used by the atomic swap system so that the currency you need to swap can be delivered within a particular duration; otherwise, it is likely to be canceled. This is done to preserve the atomicity for the swap to occur or none of the currency will be swapped.
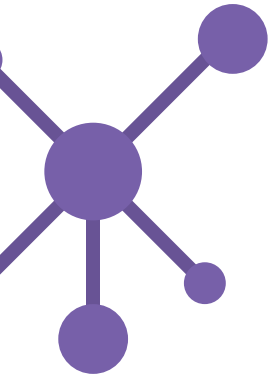
Smart Contracts

This is the pacesetter to all the oncoming DeepOnion applications as they are programs that execute what they were intended to perform. The reasoning behind DeepOnion coming up with the "Self-executing contracts" is to allow normal contracts between individuals to be converted into computer codes. The same version is then stored before being replicated on the system that is supervised by a computer network operating the blockchain. The outcome is a physical exchange of a value referred as the ledger feedback. This entails receipt of goods and services or transfer of funds.

If you find it difficult to understand the concept of smart contracts, Nick Szabo illustrates it as a vending machine— the first person to conceive the idea of the smart contracts. Basically, you would put some token in the vending machine for a snack or a cup of coffee. In this situation, we treat the token as the cryptocurrency. This means that their parties involved in the contract would have to meet certain conditions before they can execute the contract. The application of smart contracts can be done as multi- accounts that would demand a certain number of people to agree for a particular action to be performed. Also, it can be used in managing agreements between parties to a contract before the application details can be stored.

DeepOnion seeks to address the inherent loopholes of traditional crypto coins such as Ether and BTC. A typical example is an attack on The DAO (Ethereum-based smart contract), where a hacker carted away a sum of $50 million in Ether. DeepOnion is rolling out its plans on the smart contract where we will have an anonymous (Tor-based) self-executing contract that tops in the crypto space. This will be promoted largely by the TOR network ensuring that all details about contracts will be visible to all involved parties. It helps shut down all forms of prying eyes as well as the third parties.

DeepOnion smart contracts are definitely something that our community will be looking forward to despite the uncertainties surrounding this upcoming technology. It can be visualized in terms of when the development is scheduled to begin as well as the implementing code. It should act as a motivating factor for people who want to invest in Deep-Onion because it will certainly take the crypto-world by storm.

Lightning Network

Basically, the lightning is a decentralized network that enables instant payments across a wide network of participants using the smart contract functionality. Our development team is currently working towards implementing the lightning network that depends exclusively on the underlying technology used in the blockchain. It is possible to generate a secure network of participants transacting at high speed and high volume using real DeepOnion or blockchain transactions. It will be backed up by the native scripting language for the smart contract.

How it works

A ledger entry is created on the blockchain by two participants demanding both of them to sign off any spending of funds (Bidirectional Payment Channels). They go ahead to create transactions that reimburse the ledger entry to their discrete allocation but cannot be broadcasted to the blockchain.

Their individual allocations for the ledger entry can be updated by creating many transactions spending from the latest output of the ledger entry. The most recent version is the one that will be regarded as valid and will be enforced by smart-contract scripting that is blockchain-parsable. Either party has the authority of closing out the entry at any time without any custodianship or trust by broadcasting the latest blockchain version.

It is possible to determine a path that is similar to the routing packets across the network by creating a network of the two-party ledger entries. A script is used to enforce the payment that effectuates the atomicity through decrementing the time-locks (the whole payment can succeed or fail).

This results in the possibility of conducting transactions that are off-blockchain without experiencing any limitations. On-blockchain enforceability allows transactions to be made off-chain with a lot of confidence. This can be compared to how an individual carries out legal contracts with others. However, no person shows up in court every time they make a contract. The smart contract can be enforced on-blockchain by making the scripts and transactions parsable. The court is usually involved in the event of non-cooperation but the result is deterministic when it comes to the blockchain.

Features of the Future Transactions Using Smart Contracts

Instant Payments

No need to worry about the block confirmation times because of the lightning-fast blockchain payments. The blockchain smart-contracts enforce security without creating on-blockchain payments for individual transactions. The speed of payments is measured in milliseconds to seconds.

Low Cost

The lightning network exceptionally allows for low fees by settling off-blockchain and transactions. This allows for instant micropayments and other emerging use cases.

Scalability

It will have the ability to have millions of transactions per second across the entire network. Legacy payment rails are blown away by capacity as a result of many orders of magnitude. It will be possible to attach payment per click without the need of custodians.

Cross Blockchain

The heterogeneous blockchain consensus rules can result in cross-chain atomic swaps occurring off- chain. There is a high possibility of making transactions across blockchain without putting trust in the third party custodians.

DeepOnion Marketplace

DeepOnion will have its own marketplace where visitors will be able to buy products or services with ONION payment method. This will be a game-changer as we will charge no extra fees and sellers will be protected from chargebacks and other scams. This marketplace will be similar to Fiverr.com but only accept ONION as payment method. Our main priority is to protect the privacy of our users and this marketplace will be no exception.

DeepOnion Academy

DeepOnion Academy plans to inspire and create the first step to include new people and eliminate any barrier that can generate a disruptive and world-changing technology as the blockchain. The Academy videos are aimed at educating the masses by increasing general awareness and expansion for the crypto communities. It gives them the ability to reach new people through the simplest videos that have ever been done since Bitcoin came into existence. People can now understand more about the crypto world, thanks to the DeepOnion Academy videos.

The market used to be dirty garbage that would pump dump people while the cryptos were heavily abused by the short income dreamers. It is only through this education that people can end the problems and challenges they face from other leading cryptocurrencies. All crimes that were committed against cryptos including abuses and lies all happened because of lack of education about the industry. Most people usually hate what they don't understand and that is why DeepOnion saw it wise to offer skills and guidance in whichever way possible to counter negativity of cryptocurrencies.

The education project would be the greatest gift for the crypto world since we foster peace among our members and the entire DeepOnion community. We don't look forward to carrying wars, kill more people or enslave Africa and other weak countries but to recognize them as important individuals who deserve more dignity and respect in the society and the word as a whole. We set an example and we expect even a better approach from future education projects during the adoption and expansion of DeepOnion to any public.

EXAMINATION OF TECHNOLOGIES

The strength of DeepOnion rests in its multi-faceted approach to privacy and security which are manifested by the myriad of technologies that have been incorporated in its wallet and blockchain. DeepOnion has integrated a number of common technologies that are also present in other currencies (we adopt the current best practice). It also boasts several proprietary solutions that offer additional anonymity, security, and privacy as well as further the state-of-the-art.

It is necessary to understand the common technologies that are shared by all blockchain cryptocurrencies to discuss this further.
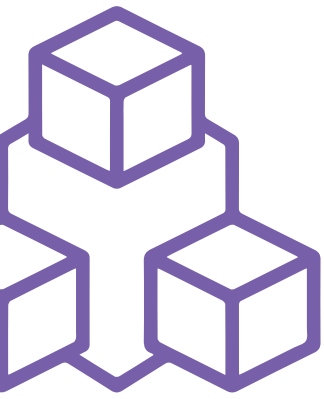
Blockchain

We can effectively define a blockchain as "continuous list of records that keeps growing" also referred to as blocks are linked and secured using cryptography. Every block incorporates a hash pointer that links to the previous block, transaction data and a timestamp. The blockchain is inherently resistant to data modification [3] by design.

One of the effective solutions to most problems that face the existing financial systems is utilizing a blockchain in a currency. An immutable public ledger is provided by the blockchain, comprising of all transactions that have transpired in the entirety of the network. This enables verification of any transactions because the inception of the coin (with the privacy trade-offs that have been described in 2.1), which makes it a simple task in the resolution of conflicts.

Blockchain Scalability

It is essential to understand the concept of throughput because the blockchain is considered to be a continuous ledger that accounts for all transactions. The maximum throughput of Bitcoin is 4 transactions per second while that of Ethereum is 7 transactions per second. The reason for this limitation is due to the amount of stored data in the blocks (block size) – records of transactions that can be stored in every fixed block size i.e. 1 MB, and the average time taken to process the hash of a block before it is added to the blockchain (block time). This can result in BTC transactions being completed in more than 24 hours. This is a fundamental flaw in a payment system that was supposed to be instantaneous. This situation has been improved by DeepOnion as many folds by integrating the PoS, faster blocktimes and larger blocksizes. This leads to a theoretical throughput of 62.5 transactions per second, detailed as follows;

1 The average size of the transaction is about 500 Bytes. The block size of DeepOnion is 1.5 MB which means that each block has the ability to hold approximately 3000 transactions.

2 DeepOnion is a hybrid coin, mixed with PoW/PoS. On average, the PoV interval is 240 seconds but the target of PoS is a lot more frequent at 60 seconds. This implies that our theoretically combined block time is 48 seconds, illustrated as (240/5).

Blockchain Scalability

For verification, we checked the blocks for the last 24 hours and this is what we get:

- Block 223460 occurs at 11:59:36 AM on 25th Nov 2017
- Block 225285 occurs at 11:59:05 AM on 26th, Nov 2017

This means;

3 In 24 hours, we have 1825 blocks which means that our average block time is set at 47 seconds, matching our designed target block time.

4 We have one block per 48 seconds with the ability to handle 3000 transactions. This implies that DeepOnion is capable of handling a maximum transaction rate of;

3000/48 = 62.5 tx/second.

This is almost 10 times of Ethereum's throughput is more suitable, scalable and effective for mass adoption as a cryptocurrency.

The transaction speed of DeepOnion can be increased further by the future implementation of the lightning network technology [8]. If not faster, this could lead to the same speed of transaction, compared to the VISA network (approximately 56 k/sec). DeepOnion will be the perfect payment platform due to the fast speeds in combination with the anonymity of the Tor network.
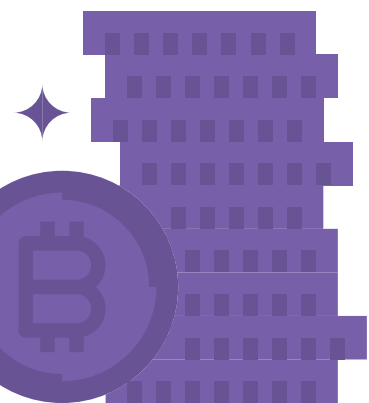
Cryptocurrency

A cryptocurrency is a digital asset that secures its transactions using cryptography and was designed to operate as a medium of exchange. It also verifies the transfer of assets [4] and controls the creation of additional units. Bitcoin was released in 2009 by Satoshi Nakamoto as the first decentralized cryptocurrency.
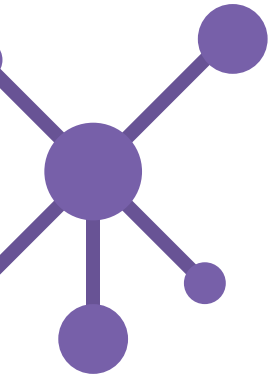
Decentralization

Decentralization is the process of dispersing or distributing powers, functions, people, or things away from the authority or central location [5].

In regards to the crypto world, decentralization can be defined as the elimination of a central processing authority (much like the VISA). Every node on the network, (a miner or typically wallet) is verified independently through a process of cryptographic hashing functions with every block within the blockchain.

This approach has the advantage of increasing the security levels on the network and reducing the reliance of putting trust on the payment processor. You would have to compromise at least 51% of the network to interfere with the process. Probably, this might not have been feasible given the different operating systems and protocols as well as the global distribution of nodes. Every node has the ability to verify new block which benefits the network. DeepOnion introduces the PoS, taking this step further than BTC which gives another form of verification and mining. This leads to the necessity of having to compromise a larger share of the network across two channels which is effectively impossible.

Although the verification of each transaction has maximum security, it also explains the reason why transactions usually take a long time compared to the traditional methods of payment. The lightning network is one of the technologies that offers an approach to solving this option of scaling. However, you will be reducing the security which reduces the number of verifications every time transactions are taken off the core. A complex problem is determining the number of confirmations or security required and one that currently is the focus of various projects such as Ethereum and BTC.

DEEPONION INNOVATION TECHNOLOGIES

In section 5, we defined the commonalities behind all cryptocurrencies. It is also important to introduce the novel blockchain technologies that will be implemented by DeepOnion to meet the dynamic demands in the cryptosphere. This involves the necessity to improve anonymity and privacy beyond current efforts.

DeepOnion is an anonymous coin that was built from Supercoin with stealth transactions that are enhanced by coin mixing processes. A solid base is provided by Supercoin on which DeepOnion could be built and improved on. The sections below will detail the novel blockchain implementa-tions of DeepOnion and the reason why they were selected.

TOR

Tor can be defined as a communication service that is anonymous, has a low latency, and is based on a circuit. The original design has limitations which are addressed by the Onion Routing System of the second generation through the addition of directory servers, exit policies that are configurable, a practical design for services, an ideal forward secrecy, integrity checking, and congestion control with a hidden location through points that are rendezvous. Tor requires no kernel modifications or special privileges because it works on the internet of the real world. It requires little coordination and synchronizations between nodes. Furthermore, it also provides a reasonable tradeoff between efficiency, anonymity, and usability [2].

This provides an ideal platform where to build an anonymous cryptocurrency. The idea of proof of stake was also precisely decided to create a safer and stable TOR network. With the mass adoption of DeepOnion, the TOR network can expand to new levels helping to create a powerful network that will make it difficult for any person to analyze the network traffic. The TOR network will also include new relay codes with any DeepOnion wallet that connects into the DeepOnion Network. Therefore, the better the adoption of DeepOnion, the safer the TOR network and both technologies can benefit from each other.

The TOR network is an open source project that has undoubtedly bad frame around the world since media exploits any resource to sell regardless of whether they are totally biased. Actually, the TOR network is the best way for many people to be heard in countries where there is a total censorship or means to report criminal activities for journalists or whistleblowers that cannot resign to their privacy for obvious reasons.

The new digital era is making clear that privacy is no longer something that we have. This is because the new gold for them is our personal information, without mentioning the number of vulnerabilities that exist in common networks – vulnerabilities that can be abused by any criminal. DeepOnion believes that the TOR Network should be used as a default or at least our privacy on the internet should be something that we can't resign. It is essential that we defend our privacy before it becomes too late.

Currently, DeepOnion is upgrading to the latest 0.3 protocol that will introduce the latest anonymous features to our wallet that are most secure to protect our users. It is also essential to emphasize that all connections arising from the DeepOnion wallet are usually made over the Tor network. Your public IP address can never be exposed at any point.

DeepSend

DeepSend is a side transaction security feature that was designed to hide traces of transactions within the blockchain (a problem identified earlier with BTC). This is distinctively different from the integration of our TOR that anonymises and secures the network traffic at the transport layer. A number of technologies that are comprised in DeepSend include;

- The Zero Knowledge technologies by Zerocoin and Zerocash such as ZCoin and Zcash
- CoinJoin technologies either with the random mixers (e.g. Supercoin and Dash).
- CryptoNote's Ring Signature such as Monero and Bytecoin.

Each technology comes with its own advantages and disadvantages. For instance, you must mint and burn new coins that are unrecognizable in Zero-Knowledge technologies since it would require an additional amount of space in the blockchain. Currently, DeepSend is programmed to become a CoinJoin and Mixer technology that is based on multi-signature technologies that are trustless. Therefore, they offer a competitive edge of privacy and anonymity. In order to conceptualize this idea, think of the following scenario;

**1**   Person A wants to pay $x amount of money to Person B

2   If Person A chose to make direct payments to Person B, then the transaction would be publicly disclosed to all (the current situation in BTC). On the contrary, Person A will pay Person C who goes ahead to pay Person D. After iterations, Person Z then pays the amount to Person B.

3   This implies that multi-signatures guarantee all payments that were done by both Person A and B, and neither of these addresses is connected to individuals.

4   The main reasoning behind this is that Person B gives money to Person C who later pays it to Person D with a different address that is unrelated. Given enough iterations, it makes it very difficult to reverse traces of the transaction.
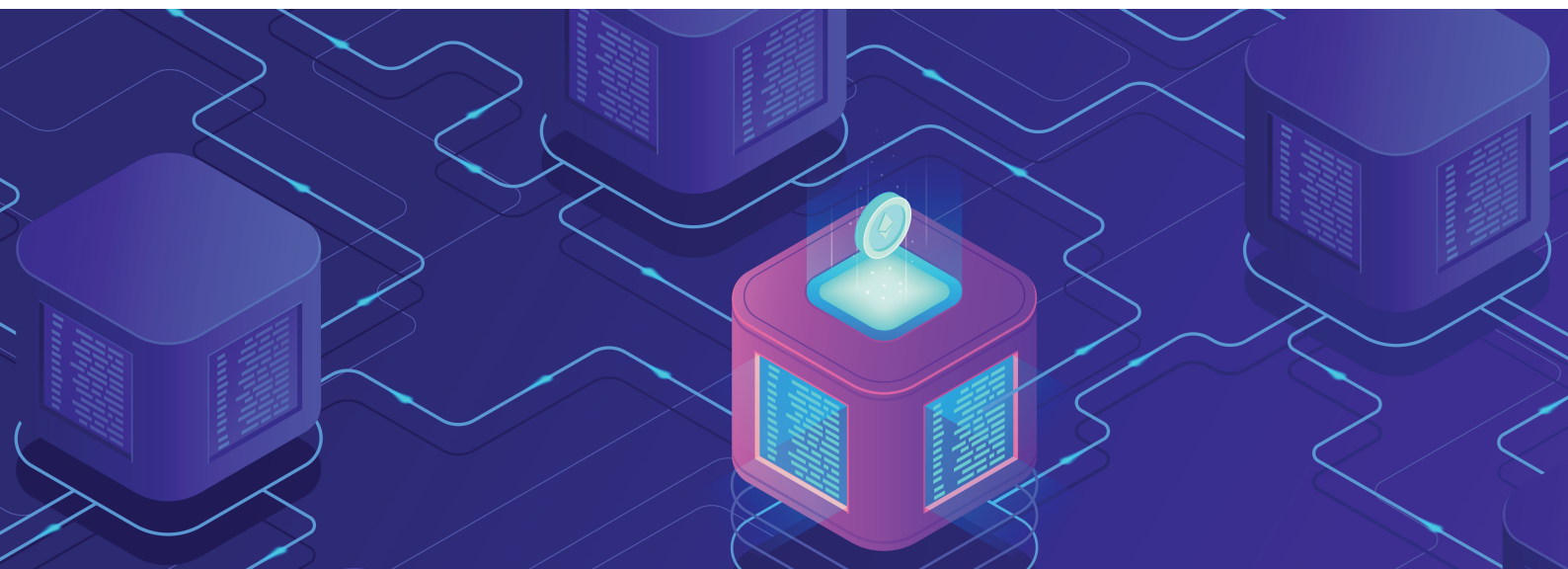
DeepSend
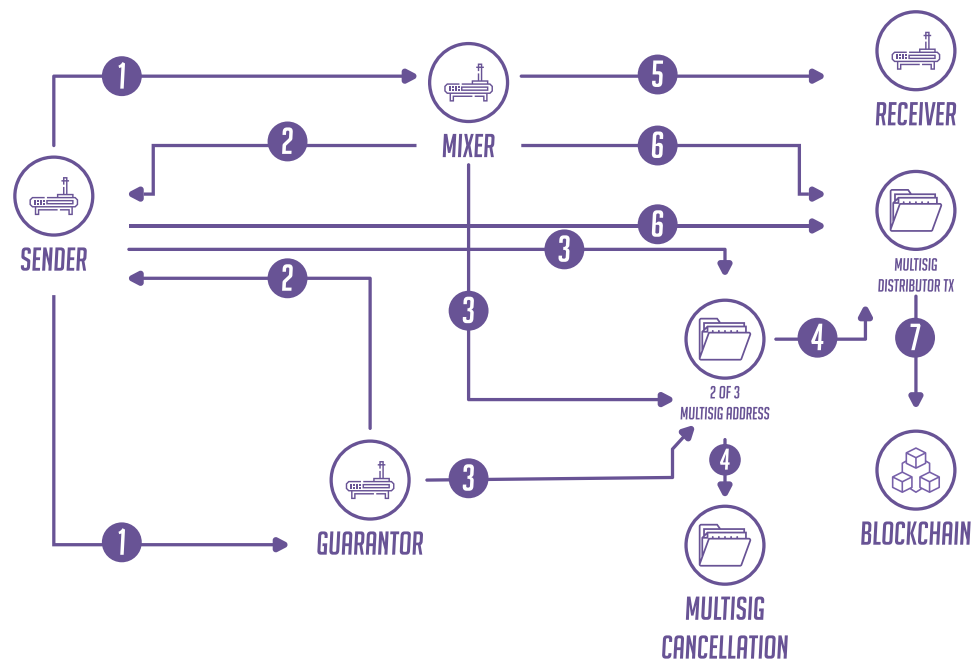
1. Sender randomly picks two nodes from his service node list, and request anonymouse service
2. Mixer and Guarantor reply favorably
3. The 3 parties exhange public keys and create 1 2 of 3 multisig address. They each deposit a guarantee fund to it. Sender also deposits the send amount and service fees
4. After verifying the deposits in escrow, a multisig distribution tx and a multisig cancellation tx will be created and sent to each party
5. After veryfying the two multisig tx, Mixer will send the required coins to destination, and send the txid to other parties to verify
6. Mixer will sign the multisig distribution tx and send it to other parties. Sender will verify Mixer's txid, if satisfied he will sign the multisig distribution tx
7. Sender will post the distribution tx to the network. All escrows are refunded, the send amount is sent to mixer, all fees are paid, and anonymous transaction complete

Fig. 3 Shows DeepSend Transaction: Obfuscation through multi-signature and Coin Join. [9]

DeepVault

DeepVault allows members of DeepOnion to store hashes of files (file validation credentials) within the blockchain. In other terms, it is a store of immutable information held within the blockchain that allows members to verify the integrity of a file over time. Therefore, you will know that the file has been corrupted or altered when the hashes of file changes. This tool will also be invaluable in determining whether your essential documents have not been tampered with and that they are secure. An obvious use for this feature is legal documents as it allows the verification of this document by the interested parties, hence the content will not be altered erroneously, maliciously or through file corruption without the consent of the person. Consider this an expansion of smart contracts where validations of integrity or conditions are done through cryptography.

- A video demonstrating all details about DeepVault has been produced by a community member. [6]
- For those who cannot view the video, a manual is also available [7].
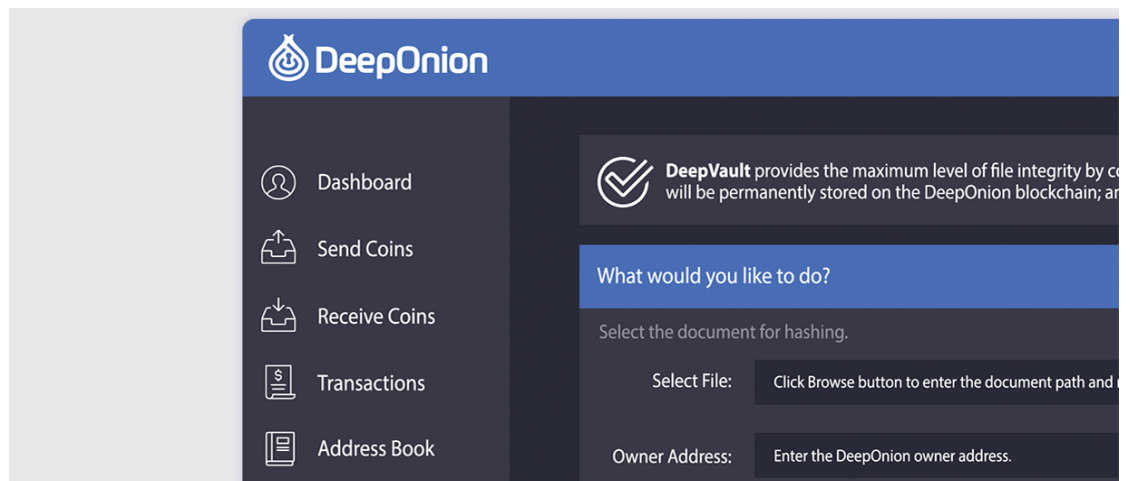
DeepVault

Fig. 4 DeepVault – DeepOnion wallet

DeepVault is highly intuitive and has been integrated into the DeepOnion wallet. It is a novel feature that offers a solution to the simple file validation which has been the major problem. The processes of file verification and hashing have been improved by DeepVault which provides several benefits that are simple to use. They are;

- Generation of the file hashes is done using a GUI that is normally embedded within the wallet.
- The SHA-256 is the secure and trusted algorithm used by the hashing process
- The file hashes are protected within an immutable blockchain by DeepVault which keeps them safe from any alterations.
- The verification of the file can be locked to the user thus preventing others from validating the file.

We believe that DeepOnion is an essential tool that facilitates our users to protect and safeguard themselves in the digital era. There are innumerable benefits that come with the ability to verify the integrity of our files and can be applied in almost every situation. The Q1 2018 marks the expansion of the DeepVault and the deployment of a non-wallet based solution that will be hosted in the cloud. It will allow the files to be secured by a web-based interface. We will soon release all details.

The upcoming DeepVault web app will also allow the registration and verification of files online. This will be a game-changer to clients of different fields that need a blockchain notary or timestamp service. The development team will also create an API which will make it possible to create a mobile app to use the DeepVault using your mobile phone. This is a feature unmatched by any of our competitors as it is built from scratch and continuously being improved. The DeepVault web app can be found at www.DeepVaultOnline.com

Mobile Wallet

The DeepOnion mobile wallet is yet to make its debut in 2018 on the Android operating system. It will offer functionality that is similar to the desktop experience (Confirmation of the final features will be communicated) and will operate naturally over the TOR network thus offering protection to your identity while on the move. DeepVault is an essential feature of the mobile wallet as it protects your documents even on the fly. It also offers a natural application for safeguarding your photos.

Furthermore, users will be in a position to view their address book, transactions and gain access to the VoteCentral. Most importantly, they will be in a position to send and receive ONION naturally.

Currently, we are in the primary stages of hiring an IOS developer who will make the mobile wallet available to the Apple devices. The branding of DeepOnion mobile wallet will be done in accordance with our website for our community to have a homogenous user experience across all platforms. One of the essential elements of our mobile wallet is the User experience which will be undergoing extensive testing that ensures the wallet offers a natural feel to any person irrespective of their experience in cryptocurrencies.

Fig. 5. DeepOnion Mobile Wallet

VoteCentral

VoteCentral is a voting platform that is open to all and was founded upon the blockchain technologies that will allow voting by the DeepOnion community on the proposals and tasks that have been suggested and submitted by the community members relating to the future trends of this project. Members will have a huge impact on the decisions made by the community that influences the DeepOnion expansion project as well as the direction taken by the development team.
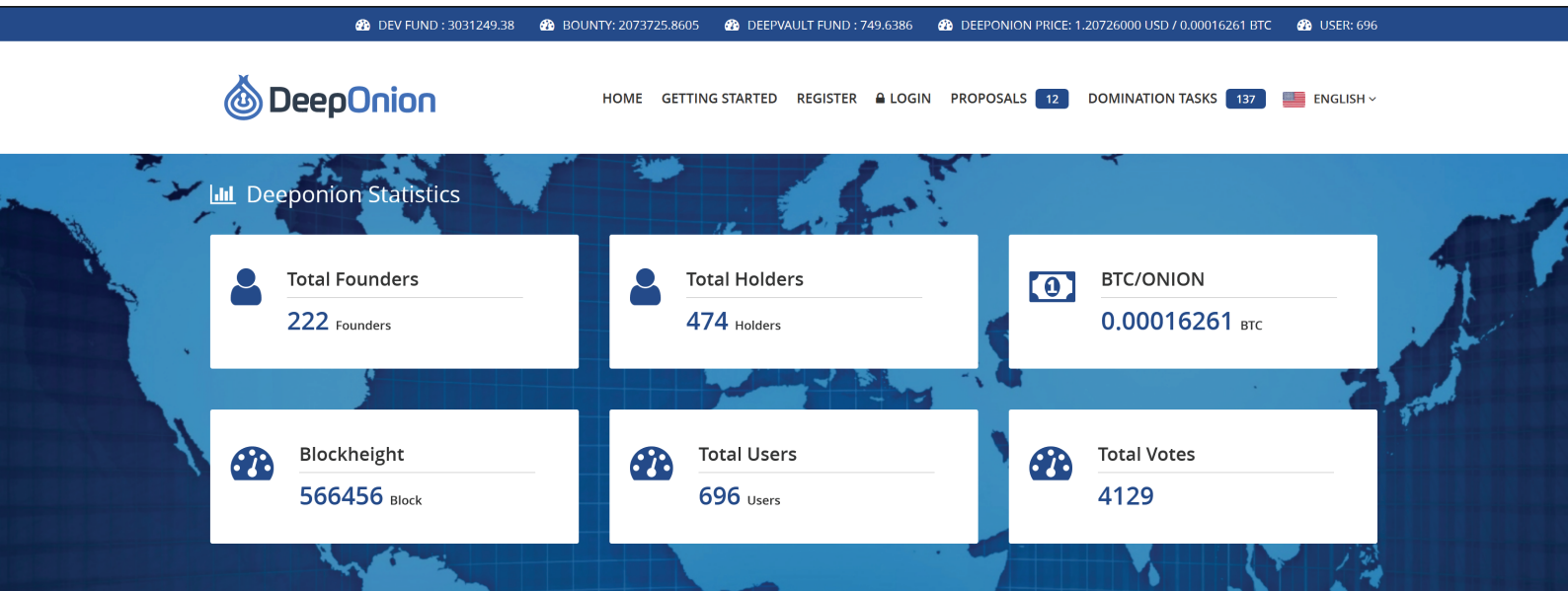

DEV FUND : 3031249.38   BOUNTY: 2073725.8605   DEEPVAULT FUND : 749.6386   DEEPONION PRICE: 1.20726000 USD / 0.00016261 BTC   USER: 696

DeepOnion   HOME   GETTING STARTED   REGISTER   LOGIN   PROPOSALS 12   DOMINATION TASKS 137   ENGLISH ⌄

Deeponion Statistics

Total Founders	Total Holders	BTC/ONION
222 Founders	**474** Holders	**0.00016261** BTC

Blockheight	Total Users	Total Votes
566456 Block	**696** Users	**4129**

Fig 6. VoteCentral – Landing Screen (In Alpha)

It contains many parallels to the existing system of democratic voting in modern politics only that it mitigates voting fraud because of the additional benefits of the blockchain technology. Community suggestions or new directions can be registered through VoteCentral before being evaluated by the Airdrop founders, Development team and the holders who have ONION balances within their wallet that are more than the necessary minimum.

As mentioned earlier, VoteCentral is considered as a layered approach. This hierarchy can be conceptualized by imagining three concentric circles:

1 The core, which is the inner circle, consists of our initial founders and development team.

2 The surrounding core refers to our airdrop founders who are mandated with the right to vote in the VoteCentral.

3 Lastly, the exterior is comprised of long-term DeepOnion supporters, as well as participants who have made massive contributions towards the DeepOnion project.

Voting is based on a member's status that was granted through long-term support (or proven contributions to the community). At this point, the voting power (vote weight) of the member depends on the balance in their ONION wallets.

VoteCentral

There are two phases of the VoteCentral, which includes a centralized solution that is supported by the web technologies and the next phase of the future that will be supported by the blockchain. This software will be used by wallet owners to the suggested proposals of the community as well as the tasks submitted, based on the number of ONION that they hold within their wallets.

In the first phase, we request a proof of ownership from our participants through registration of a signing message. We can check the wallet address of a member every day and make a decision on their voting power with regards to the proposals suggested, awaiting the decision from our Development team or others. Proposals will be required to meet standards that have not been defined yet and should also follow protocols. However, this will be defined at a later date.

Our Founders, Development team, and the future Holders will have the ultimate decision in the VoteCentral on the direction to be taken by the project. However, each circle of members will be in a position to express their sentiments.
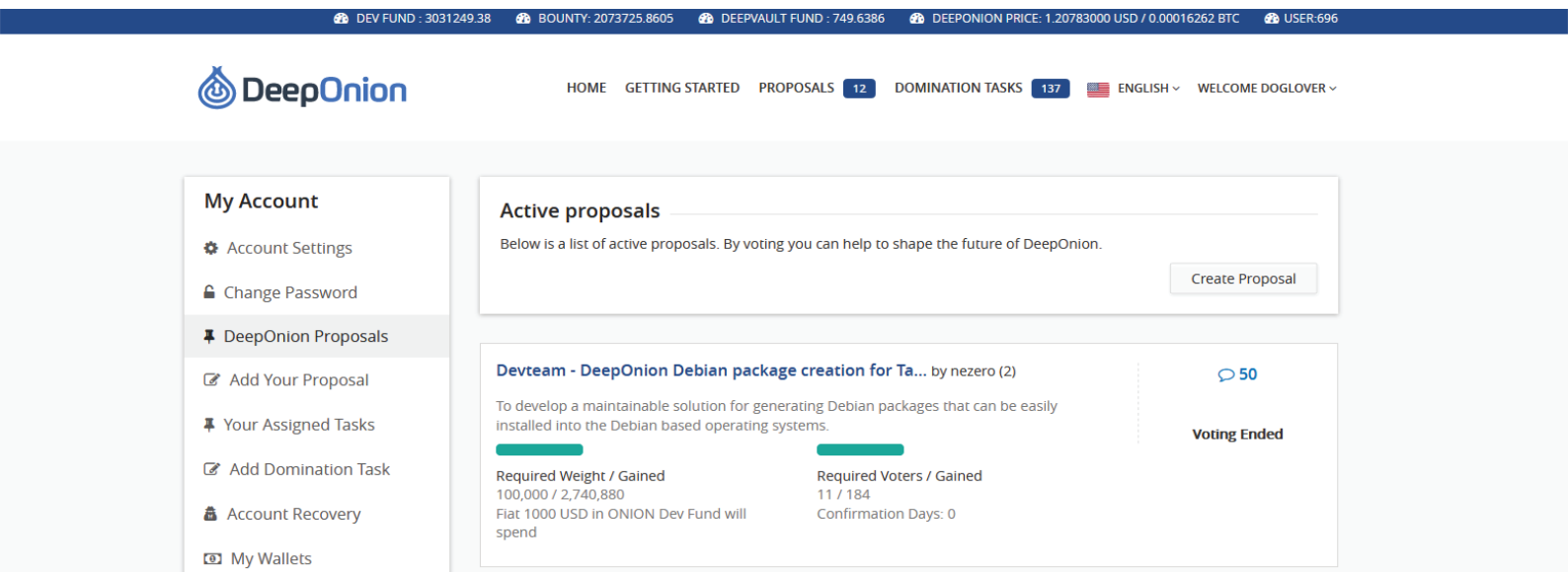

Fig 7. Viewing and Creating Proposals – (In Alpha)

We are looking to establish a 'living organism' because of our grand ambitions with VoteCentral where we can accept or reject decisions depending on a process of robust analysis and evaluation that is supported by the sentiments from our community and weighing in a democratic arena.

We select the best proposals and tasks that are most popular from VoteCentral before using them to guide the future domination (expansion) of the DeepOnion project. By proving your commitment to DeepOnion, you play a pivotal role in our future as you can raise your opinions, which ultimately rewards you with a higher voting weight within the project. We believe that DeepOnion will become stronger the more we build our Founding community.

DeepPoints

The reward program for our community is referred to as DeepPoints which allows members to earn ONION because of their massive contribution towards the project. Our primary goal is to reward members who contribute meaningful posts on a regular basis as well as promotional materials that would benefit the wider community. A Public hero will be added (this person will attend the blockchain conferences and be a YouTube Cryptocurrency celebrity).

Their main purpose will be to boost the DeepOnion brand name. DeepPoints has flexible and dynamic criteria, a model that suits the rapid development experienced by DeepOnion as well as the spontaneous real of cryptocurrencies. Our ability to target our whole community and adapt to a specific objective or goal portrays the strength of this approach. There are many attempts where this has turned out to be successful with regards to the exchange listings such as the Satoshi Exchange and the KuCoin. There are no doubts that our expansion will extend to the Binance and Bittrex platforms.

It is quite simple for our members that the more you complete Official tasks of DeepOnion (Domination), the more replies, likes and threads you accrue (inside of the documented rules whilst avoiding spamming), and the more you will receive the DeepPoints. Most importantly, you get a reward of 5x the standard remuneration of replies and likes (Those that were specifically designed for the mod/development team to target a particular objective).

2% to 10% of the distribution within our weekly airdrop is reserved for the DeepPoints rewards. This provides a real opportunity where our community can earn lucrative rewards due to their participation. It is also a perfect opportunity for our loyal followers to be rewarded by the DeepOnion team.

E-commerce plugins

Our development team is currently working on producing a number of plugins where ONIONs can be used as a method of payment. WooCommerce is an open-source e-commerce plugin that has now been released. It was specifically designed for WordPress. Over 380,000 online retailers have already adopted this plugin and are also used by a number of heavy traffic websites. There is a large number of users in WooCommerce which makes it ideal for the currency to be accepted as a method of payment on this platform.
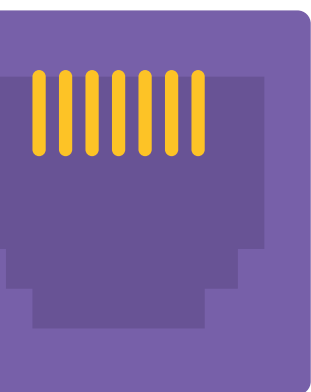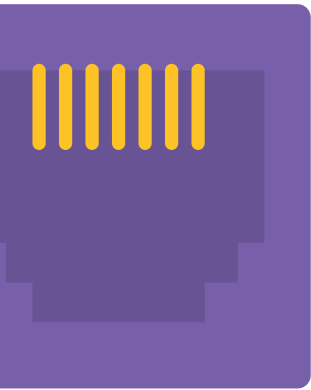
E-commerce plugins

Other plugins being developed include OpenCart and PrestaShop. OpenCart is an online store management system that supports many different currencies and languages, and it is also freely available. PrestaShop is a premium open source e-commerce solution available in 60 different languages and 250,000 shops worldwide. Behind all these solutions, DeepOnion will be making plugins for some of the major e-commerce platforms such as Shopify, Magento and much more.

There will no longer be restrictions with the DeepOnion plugins since owners of Onion currency will be able to carry out their payments in any part of the world.

Today, you can sell online with DeepOnion by accepting the Onion currency on your online store. The development team is also working on a new web design and a page that will provide necessary support to all e-commerce users at no cost. DeepOnion is yet to take the anonymous cryptocurrency payment acceptance market. This is an effort to stop credit card fraud and chargeback scams by making instant payments. You won't have to wait for weeks or months to get paid.

Trezor Hardware Wallet Compatibility using the Electrum Wallet

Trezor is a single purpose device that allows crypto-investors to make secure transactions. Transactions remain completely safe despite being initiated on a vulnerable or compromised computer. We believe that the use of Trezor hardware wallet compatibility will help DeepOnion adoption among people who are not familiar with security procedures.

It works when DeepOnion protocol sends signed notes of payment via the internet. A special algorithm is used to sign the transactions which require a unique key or password. The key is held in Trezor hardware wallet as it was specifically designed to help you sign transaction messages securely. Trezor can be thought of as the modern-day stamp in crypto-world. Every Trezor comes with its own PIN code which makes it impossible for any person to access your account. Hackers may compromise the computer where you use your Trezor but they will never get hold of your key.

Trezor Hardware Wallet Compatibility using the Electrum Wallet

DeepOnion will be among the top cryptocurrencies that use Trezor hardware wallet compatibility to ensure the privacy and anonymity of its users. It supports Windows 7 and other higher versions as well as Linux and OS X versions. Trezor can also be used with other Android devices that have USB Host. Firefox and Chrome ate the major supported browsers of the Trezor wallet. Although you can use other browsers, we cannot guarantee their full functionality.

Trezor hardware wallet compatibility will be the most secure and trusted way to store your ONIONs using the Electrum wallet. You can now enjoy DeepOnion without risk by isolating your private keys into safety with the Trezor hardware wallet.

Features of Trezor hardware wallet

- It has a reliable hardware, advanced cryptography, and simple interface.
- It is small and sturdy
- It is water resistant, tamper-proof and extremely durable
- It allows for minimalistic operations
- It allows checking of essential transaction details before confirmation.
- It has a powerful cryptography
- Everything important requires a direct physical approval of the user.
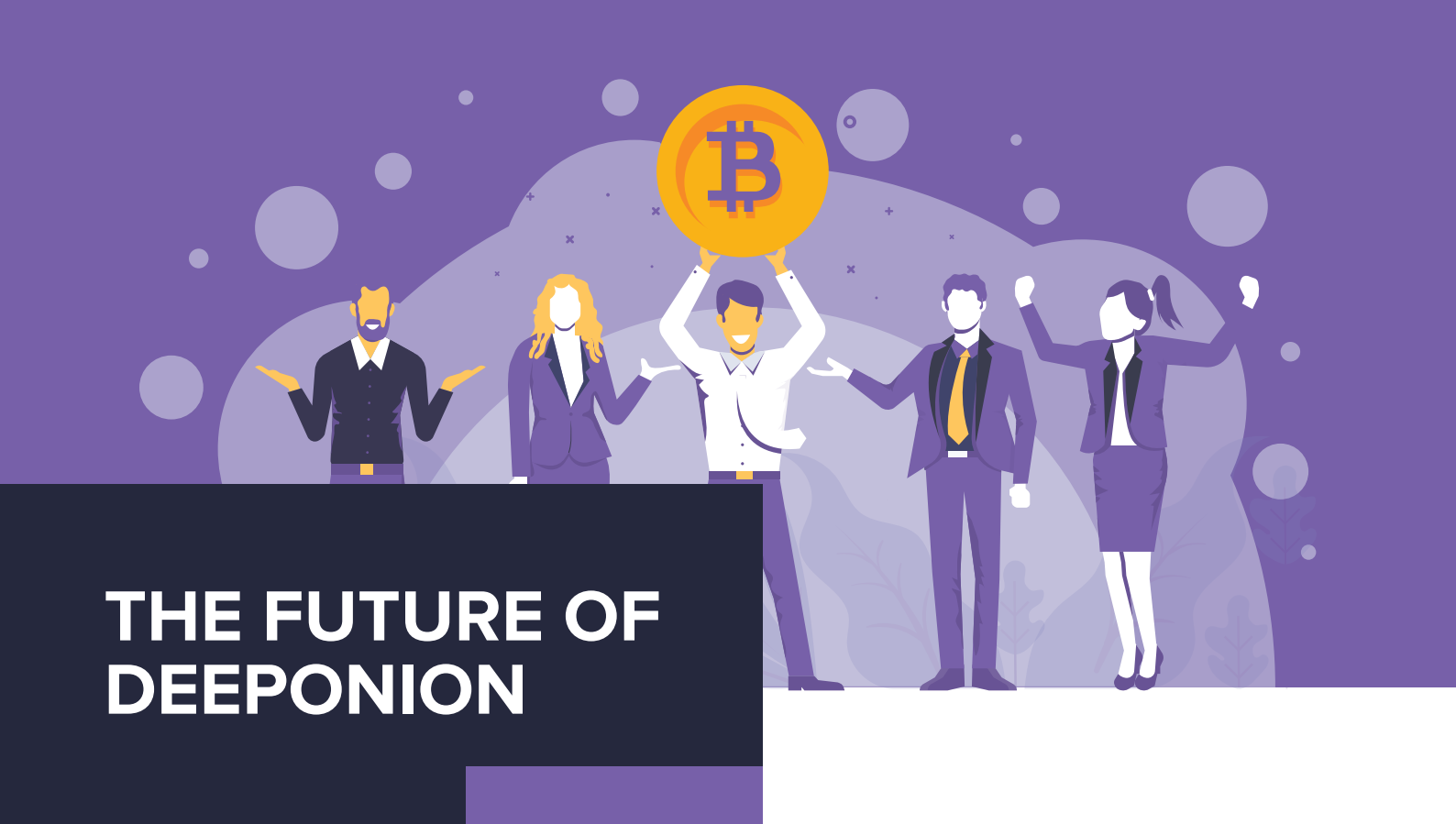
THE FUTURE OF DEEPONION

DeepOnion takes pride in 2017 as a tremendously successful year for the development team and the members of the community. We are one of the most popular forum threads you can find on BitcoinTalk.org and have done that in a period of more than 6 months as a community. We have visualized a strong growth on our forums of approximately 14,000 members with strong mining that will support our blockchain. 2018 is set to be the year of breaking records following the recent expansion of our development team and our current roadmap.

We are contacted by major investors and exchanges on a daily basis for listing while the prominent crypto celebrities wish to take part in the DeepOnion project. We are humbled to see that all the hard work from the Development team and members of our community is yielding results. Our development team is currently working on the Electrum Wallet and ledger compatibility and the main DeepOnion Wallet will soon have different style themes.

It is essential to emphasize that we will soldier on until DeepOnion becomes the adopted de-facto privacy cryptocurrency. Our exchange listings and trade volumes continue to grow on a monthly basis. Our message is spreading rapidly across the world as we continue to integrate our novel blockchain technologies. As denoted in our roadmap, we haven't even begun our advertising campaign. We are very confident as the development team that DeepOnion will be propelled to the forefront of cryptocurrency adoption with a celebrity endorsement and a fully implemented roadmap.

2018 will be a year of excitement for members of DeepOnion community. Here are the features that are to be implemented as mentioned earlier;

- DeepSend
- DeepVault Website
- VoteCentral
- Mobile Wallet
- Smart Contracts
- Atomic Swaps
- Celebrity endorsements
- Advertising Campaign
- DeepOnion Academy
- Ecommerce Plugins
- Tier-1 Exchanges

Appendix A

- Airdrop Specification
- Total Premined 18,000,000

  - 3,200,000 Airdrop Rounds 1-15
  - 6,800,000 Airdrop Round 16-40
  - 250,000 each on Round 16 – 30
  - 300,000 each on Round 31 -39
  - 350,000 on Round 40

Furthermore, 10% of the airdrops will be used for events in the DeepOnion forum each week to reward any participation at the forum community of DeepOnion. The remaining 90% is often airdropped directly.

Bounty Fund: 3,000,000

The balance currently stands at 2,600,000 after the various events, distributions, bounties, and rewards. This fund is usually channeled to reward contributions such as videos, articles and significant contributions that are beneficial to DeepOnion and members of its community. It will also provide support to potential new merchants to choose DeepOnion.

Founders reward: 2,000,000

Development fund: 3,000,000

For example, new feature developments and smart contracts. VoteCentral will determine how these funds are used.

Acknowledgments

The DeepOnion development team would like to appreciate our community and all participants who have offered us support throughout our journey. This project has thrived from its roots because of your efforts and involvement. Although we have the vision and technology, you are the ones who assist us to distribute this into an ecosystem that is workable. We all benefit from private and anonymous financial transactions in a world that are increasingly dominated by the pervasive digital espionage. We highly thank you for your continued support and we urge you to continue with the same spirit.

The DeepOnion team would also like to recognize the ongoing work of their diligent Moderator team who have achieved massive success in fulfilling the requirements of the project as well as the Deep-Onion community even through the festive season.

We send a special thank you to the community members for the provision of graphics that have been included in the white paper

DeepOnion is not just something written on a stone since we can improve and add more features to our project. We are evolving all the time as any other open source project that includes people from any part of the world.

Glossary

Whitepaper: It is a report that gives well-documented information or proposals regarding a specific project (e.g. the DeepOnion Project and upcoming features.)

Proof of Stake (POS) — It is a concept where a person can mine block transactions or validate them depending on the coins that they hold. This implies that the more ONIONs or altcoin you own as a miner, the more mining power you will have.

Proof of Work (POW) — This is an economic measure that limits the denial of service abuses or attacks and requires work from the person requesting the service. It simply refers to the processing time by a computer.

Blockchain- It is the world's leading software technology that is used to build a better financial system in cryptocurrencies.

Decentralized — It refers to shifting of departments from one administrative location to other centers.

Hash — It involves taking any length of an input string and giving out an output of a specific length. Transactions are considered to be an input that is run into a hashing algorithm e.g. the SHA-256 that gives a fixed length of output.

Stake - It is the act of holding a cryptocurrency in your wallet for a fixed period of time to accrue some interest.

TOR: It can be defined as a communication service that is anonymous and has a low latency based on a circuit.

Cryptocurrency - It is a digital currency that modulates the creation of currency units and allows verification of fund transfers using encryption techniques. It doesn't require intermediation by the Central bank.

DeepVault - it is a store of immutable information held within the blockchain that allows members to verify the integrity of a file over time.

DeepSend — It is a side transaction security feature that was designed to hide traces of transactions within the blockchain.

Privacy — It is the ability of a person to selectively express themselves by secluding any information about themselves. DeepOnion is a cryptocurrency that guarantees the privacy of its users.

Anonymity- The quality or state of being unknown to most people: the quality or state of being anonymous.

References

[1] The Bitcoin Project. 2017. Bitcoin is an innovative payment network and a new kind of money. Available at: https://bitcoin.org Last Accessed: 31/12/17

[2] R. Dingledine, N. Mathewson & P. Syverson. 2013. Tor: The Second-Generation Onion Router, 2nd ed. Available at: https://svn.torproject.org/svn/projects/design-paper/tordesign.pdf.

[3] Economist Staff Blockchains: The great chain of being sure about things. Available at: https://www.economist.com/news/briefing 21677228-technology-behind-bitcoin-lets-people-who-do-not- know-ortrust-each-other-build-dependable, 31/10/2015.

[4] A. Greenberg. 2011. Crypto Currency. Forbes.com. Available at: https://www.forbes.com/forbes/2011/0509/technologypsilocybin- bitcoins-gavin-andresen-crypto- currency.html.Retrieved 12 December 2017.

[5] Definition of decentralization. Archived 2013-01-26 at the Wayback Machine., Merriam-Webster Dictionary, accessed February 4, 2013.

[6] Community member. 2017. DeepVault Tutorial Video. Available at: https://deeponion.org/community/threads/deepvault-videoguide.3780/.

[7] Jimmybob. 2017. DeepVault Tutorial Manual. Availableat:https://deeponion.org/community/threads/tutori aldeepvault. 3868/.

[8] J. Vermeulen. 2017. 'Bitcoin and Ethereum vs VISA and PayPal',Available at: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions- persecond.html Last accessed: 28/12/17.

[9]SuperCoin.2016'SuperCoin's Revival'. Available at:https://bitcointalk.org/index-.php?topic=1351548.0 Last Accessed:28/12/17

[10]Wikipedia. 2017. wannacry Available at:https://en.wikipedia.org/wiki/WannaCry ransomware attackLast Accessed: 01/01/18

[11] M. Green. 2014. 'Zero Knowledge Proofs:An Illustrated Primer'. Available at: https://blog.cryptographyengineering.com/2014/11/27/zeroknowledge-proofs-illustrated-primer/ Last Accessed: 01/12/17

[12] Bitcoin Wiki. 2018. 'Multisignature'. Available at:https://en.bitcoin.it/wiki/Multisignature Last Accessed:01/01/18

[13] Wikipedia. 2018. 'Collision Attack'. Available at:https://en.wikipedia.org/wiki/Collision attack Last Accessed:09/10/17

Our Team

Deeper

Community Manager + Marketing

Deeper is an experienced project manager with a strong knowledge of marketing. Experience in development.
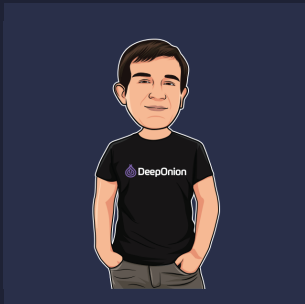
Monocolor

Lead Blockchain Developer

Monocolor is the lead blockchain developer & has many years experience in C++ and various programming languages.

Nezero

Mobile App + Blockchain Developer

Experienced blockchain and mobile application developer. Nezero developed our Android mobile wallet.

Impressive

Web App Developer + Designer

Web Application Developer, Graphic Artist, UI/UX Designer, Web Designer and Crypto Enthusiast.
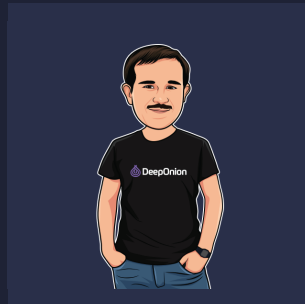
DogLover

Web App Developer + Designer

A web application developer, graphic designer, and a SEO/SEM expert with 17 years experience.

Sean

Blockchain Developer

A blockchain developer that is dedicated to the team. Working on several important additions to the DeepOnion wallet.

Dan Damian

Blockchain Developer

An experienced software developer and expert in C++. Experienced user interface software integration.
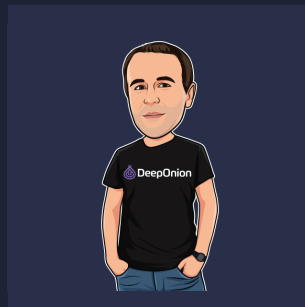
Airtorp

Blockchain Developer

An experienced blockchain developer specialized in C++ and many other programming languages.

Our Team
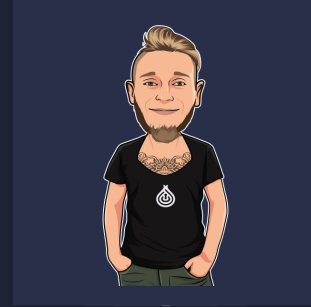
Kubera

DeepOnion Public Hero

Our first public hero. Kubera will be our speaker at blockchain events. Also has an extensive YouTube channel and fan base.

MrChef111

Lead Video Developer

MrChef produces several professional videos for DeepOnion. He has many years of experience in video production.

Knepala

Marketing Professional

Experienced with online and social media marketing. A respected member and always eager to help with marketing.

Iamgroot

Lead Marketing Manager

Experienced marketing manager. Behind the scenes marketing for DeepOnion. Also a web developer.

Our Team

Bykardinal
DeepOnion Moderator

In charge of bounty payments, VIP payments and more. Bykardinal is a respected moderator of our community.

EscapefromFreedom
DeepOnion Moderator

Professional Russian translator. Software update testing and one of our technical support specialists.

Vaas
DeepOnion Moderator

Professional Spanish translator, support specialist and working on several behind-the-scenes contributions.

Nicolas
DeepOnion Moderator

Experienced moderator and Spanish translator. Translates all news and updates to the Spanish community.

Seele
DeepOnion Moderator

German translation and wallet testing. Experienced moderator and support specialist.

Crypto Vokain
Video Producer + Moderator

Video producer, community engagement, support specialist and working on several behind-the-scenes projects for DeepOnion.

Mos
DeepOnion Moderator

Chinese community manager. Experienced in Chinese translation and in charge of contacting Chinese exchanges.

Cobaro
DeepOnion Moderator

Chinese community moderator. Pengbin provides support and community engagement in the Chinese forum.

Pengbi
DeepOnion Moderator

Chinese community moderator. Pengbin provides support and community engagement in the Chinese forum.

WhoKnows
Tech Support + Full-stack Developer

All around technical support. Experienced in full-stack development and makes several behind-the-scenes contributions.